FILED
2022 May-04 PM 01:34
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

Shymikka Griggs, *individually and on behalf of all others similarly situated*, Plaintiff, v. NHS Management, LLC, Defendant.	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Shymikka Griggs, individually and on behalf of all others similarly situated, brings this action against Defendant NHS Management, LLC ("NHS" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of a "sophisticated cyberattack" perpetrated against Defendant NHS, a consulting firm that provides management services for nursing homes and physical rehabilitation facilities in Alabama, Arkansas, Florida,

and Missouri, that occurred between February 25, 2021 and March 16, 2021 (the "Data Breach"). The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information.

2. As a result of the Data Breach, Plaintiff and an as-of-yet undisclosed number of putative class members[1] suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. The personal information compromised in the Data Breach included, *inter alia*, the full names, dates of birth, Social Security numbers, medical information, and health insurance information of NHS's current and past employees and vendors, as well as the patients/residents of the facilities it serves and their family members and guardians ("Class Members"), each of whom received a belated notice of the Data Breach from NHS ("Notice Letter"[2]).

4. Health care-specific data, which was compromised in NHS's Data Breach, is protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and information such as

[1] *See Cases Currently Under Investigation*, Office for Civil Rights, U.S. Dept. of Health and Human Services ("HHS"), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 2, 2022). Upon information and belief, NHS's claim of "501 affected individuals" is a place holder and does not accurately reflect the number of individuals affected.
[2] *See, e.g.*, Plaintiff's Notice Letter, attached as Exhibit A.

Plaintiff's and Class Members' Social Security numbers is deemed personally identifiable information ("PII") (collectively, "Personal Information").

5. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of a third party.

6. Upon information and belief, Defendant maintained the Personal Information in a reckless manner. As evidenced by the Data Breach, the Personal Information on Defendant's computer system and network was maintained in a condition vulnerable to cyberattacks.

7. The potential for a cyberattack and subsequent improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Personal Information from the risk of a cyberattack.

8. Plaintiff's and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the PII and PHI that NHS collected and maintained is now in the hands of data thieves.

9. Armed with the Personal Information accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently

applying for unemployment benefits, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

10. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. As a result of Defendant's actions and inactions, as set forth herein, Plaintiff and Class Members must now and in the future closely monitor their financial and medical accounts and information to guard against identity theft, among other issues.

11. Plaintiff and Class Members have and may in the future incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

12. Plaintiff and Class Members have and may in the future expend time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

13. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII and PHI was accessed during the Data Breach, identifiable by the list of individuals to whom NHS Management has sent or has attempted to send a Notice Letter.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserts claims for negligence, negligence per se, breach of implied contract, invasion of privacy, unjust enrichment, breach of confidence, and breach of fiduciary duty.

PARTIES

17. Plaintiff Shymikka Griggs is, and at all times mentioned herein was, an individual citizen of the State of Alabama residing in the City of Birmingham in Jefferson County.

18. Defendant NHS Management, LLC is a Limited Liability Company established in 2002, pursuant to the laws of the State of Delaware. It provides administrative and consulting services for individual nursing home and physical rehabilitation facilities in four states. NHS maintains its principal place of business at 931 Fairfax Park, Tuscaloosa, Alabama 35406. According to the Alabama Secretary of State's records, NHS can be served through its registered agent, Edward R. Christian, at 420 N 20th Street STE 3100, Birmingham, AL 35203.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the proposed Class are citizens of states different from Defendant.

20. This Court has personal jurisdiction over Defendant NHS as its headquarters are located in this District, it regularly engages in business with citizens of Alabama, and it provides administrative and consulting services for approximately thirty-five healthcare facility locations in Alabama rendering the exercise of personal jurisdiction by this Court proper and necessary.

21. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to these claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant NHS Management provides administrative services for skilled nursing and physical rehabilitation centers. Those services include operational expertise, financial analysis, clinical expertise, business office support including accounts payable, purchasing, marketing, technology, human resource systems such as payroll, and strategic planning.[3]

23. According to its website, NHS provides these services to numerous facilities in four states: Alabama (35 facilities), Arkansas (5 facilities), Florida (5 facilities), and Missouri (5 facilities).[4]

24. As it conducts its business, at each of its facilities, NHS collects highly sensitive PII and PHI from its employees and vendors, as well as from the patients/residents of the facilities NHS serves and their family members and

[3] https://www.nhsmanagement.com/what-we-do/ (last accessed May 2, 2022).
[4] *See* https://www.nhsmanagement.com/find-a-location/alabama/; https://www.nhsmanagement.com/find-a-location/arkansas/; https://www.nhsmanagement.com/find-a-location/florida/; and, https://www.nhsmanagement.com/find-a-location/missouri/ (each last accessed May 2, 2022).

guardians. If any of these groups refused to provide the required PII or PHI, upon information and belief, NHS is unlikely to employ the individual or vendor, or unwilling to admit the patient/resident.

25. In the ordinary course of doing business with Defendant, the above listed individuals were required to provide (and Plaintiff and Class Members did in fact provide) NHS with Personal Information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Driver's license number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Health information;
- Information concerning patient/resident's doctor, nurse or other medical providers;
- Photo identification;
- Employer information;
- Payment information; and,
- Similar information for patient/residents' family members or guardians.

26. Although NHS claims in its Notice Letters that it "take[s] take the privacy and security of personal information seriously,"[5] NHS does not follow industry standard practices in securing PII and PHI. On information and belief, NHS inadequately trains its employees on cybersecurity policies, fails to enforce those policies, or maintains unreasonable or inadequate security practices and systems.

The Data Breach

27. On or about May 16, 2021, NHS discovered that it was the victim of what it refers to as "a sophisticated cyberattack." In its "Notice of Data Privacy Event" ("Notice"), posted online and similar to the Notice Letters received by Plaintiff and Class Members, "NHS immediately took steps to stop the attack and mitigate the harm."[6]

28. Defendant engaged a forensic investigation firm to determine the nature and scope of this incident and to "restore functionality to impacted systems."[7]

29. Defendant determined that an unauthorized person or people accessed NHS's computer systems between February 25, 2021 and May 16, 2021, and at during that ***eighty day period,*** was able to access a broad cache of Personal Information it had stored there.

[5] *See* Plaintiff Grigg's Notice Letter, Exhibit A.
[6] Notice of Data Privacy Event, available at: https://www.nhsmanagement.com/wp-content/uploads/2022/04/Notice-DataPrivacyEvent_47007121_3.pdf (last accessed May 2, 2022). *See also* Plaintiff Grigg's Notice Letter, Exhibit A.
[7] *Id.*

30. By February 4, 2022, ***about a year*** after the Class's Personal Information was first accessed by cybercriminals, the forensic investigation team identified that the following Personal Information was breached: an individuals' name; address and other contact information; Social Security number, date of birth, and/or driver's license number (collectively, "PII"); as well as medical history; treatment or diagnosis information; health information; health insurance information (collectively, "PHI"). Not all information was stored or accessed for every victim (Class Member) of the Data Breach.[8]

31. Defendant's investigation further determined the individuals whose Personal Information was accessed included: current and former employees and vendors, as well as the patients/residents of the facilities NHS serves and their family members and guardians.[9]

32. NHS notified the U.S. Department of Health and Human Services ("HHS") on October 29, 2021, over ***5 months after*** discovering the Data Breach, that *at least* 501 individuals were affected when its computer network was hacked. If a breach affects 500 or more individuals, covered entities, including NHS, must notify HSS "without unreasonable delay and *in no case later than 60 days following a breach.*"[10] (Emphasis added).

[8] *Id.*
[9] *Id.*
[10] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed May 3, 2022).

33. Upon information and belief, NHS did not *begin* notifying the Data Breach victims (*i.e.*, Class Members) until on or about March 31, 2022, over a year after the Data Breach began and ***ten and one-half months*** after it first learned of the Data Breach. This delayed notice violates Breach Notification Rules, which requires that "individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach."[11]

34. NHS's investigation revealed that at least 501 individuals were impacted by the Data Breach, but to-date, NHS has not updated the HHS Portal with the final number of individuals whose Personal Information was assessed.[12]

35. Defendant explicitly admits that the PII and PHI of Plaintiff and Class Members that was accessed without authorization.

36. Defendant has obligations created by HIPAA, industry standards and common law to keep Class Members' Personal Information confidential and to protect it from unauthorized access and disclosure.

37. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

[11] *Id.*
[12] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 2, 2022).

38. Cyberattacks, such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

39. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and the data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of cyber-attacks and data breaches;

b. Failing to adequately protect the Personal Information of its current and former employees and vendors, as well as the patients/residents of the facilities NHS serves and their family members and guardians;

c. Failing to properly monitor its own data security systems for existing intrusions to enable it to quickly stop any attack and mitigate the harm;

d. Failing to ensure that vendors with access to NHS's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules

regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption);

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

o. Failing to adhere to industry standards for cybersecurity.

40. As the result of its inadequate security and procedures, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Personal Information.

41. In its Notice Letters to Plaintiff and the Class, NHS admits that after the Data Breach it has begun "reviewing and enhancing its existing policies and procedures to reduce the likelihood of a similar future event."[13] These measures could have—and should have—been in place prior to the Data Breach, and likely could have prevented the Data Breach from occurring.

42. Despite its lag in notification of the Data Breach that affected current and former employees and vendors, as well as the patients/residents of the facilities NHS serves and their family members and guardians, NHS offered victims of the attack just 12 months of identity theft services through Kroll. These services include 12 months of monitoring, fraud consultation, and identity theft restoration.

43. Based on the Notice of Data Breach letters she received, which informed Plaintiff that her Personal Information was "accessed," Plaintiff reasonably believes her Personal Information was stolen from Defendant's network in the Data Breach and was sold on the Dark Web.

44. Further, the removal of the Personal Information from Defendant's system – information that included full names, dates of birth, and Social Security

[13] *See, e.g.*, Plaintiff's Notice Letter, attached as Exhibit A.

numbers (which are the keys to identity theft and fraud) demonstrates that this cyberattack was targeted.

45. Due to Defendant's insufficient security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with the risk the misuse of their Personal Information for years.

Data Breaches Increase the Risk of Fraud and Identify Theft for Individuals

46. Cyberattacks against hospitals and healthcare organizations such as Defendant are targeted. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across US healthcare organizations. Significant security incidents are a near-universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[14] Healthcare facilities "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and

[14] https://www.himss.org/himss-cybersecurity-survey (last accessed May 2, 2022).

credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[15]

47. Defendant had clearly-defined and mandatory obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

48. Plaintiff and Class Members provided their Personal Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

49. Defendant's data security obligations were particularly important given the substantial increase in data breaches, and particularly data breaches in the healthcare industry, preceding the date of the breach.

50. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread.

[15] Eyal Benishti, How to Safeguard Hospital Data from Email Spoofing Attacks, Chief Healthcare Executive (April 4, 2019) at: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed May 3, 2022).

51. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[16]

52. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[17]

53. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[18]

54. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[19]

55. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including NHS.

56. Cyberattacks such as the one against NHS are especially problematic because of the disruption they cause to the daily lives of victims affected by the Data Breach.

[16] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed May 2, 2022).
[17] *Id*.
[18] *Id.* at p. 15.
[19] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed May 2, 2022).

57. Other security experts agree that when a cyberattack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[20]

Defendant Failed to Comply with FTC Guidelines

58. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[21]

60. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming

[20] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed May 2, 2022).
[21] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 2, 2022).

traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[22]

61. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data (like the Personal Information in this matter), treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. These FTC enforcement actions include actions against healthcare entities like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were

[22] *Id.*

unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

64. Defendant failed to properly implement basic data security practices.

65. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the PII and PHI of its employees and vendors, as well as the patients/residents and their family members and guardians constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

66. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII and PHI of its employees and vendors, as well as the patients/residents and their family members and guardians. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

67. As noted above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

68. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting

which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

69. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

70. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

71. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

Defendant's Conduct Violates HIPAA

72. HIPAA requires covered entities and the business associates of covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

73. Defendant NHS is a business associate of a "covered entity" under HIPAA. Business associates of covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical and administrative components.

74. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

75. NHS experienced a breach as defined by the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which

compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

76. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate NHS failed to comply with safeguards mandated by HIPAA regulations.

Identity Theft is Costly for Victims

77. In 2007, the United States Government Accountability Office released a report regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[23] Its warnings and recommendations are even more applicable now as the incidence of identity theft rises each year.

78. Victims of a data breach are exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the data on the black market where other thieves take over victims' identities to engage in illegal financial transactions under the victims' names.

79. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take

[23] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last accessed May 3, 2022).

on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

80. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit and correcting their credit reports.[24]

81. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

[24] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 3, 2022).

82. PII/PHI is a valuable property right, and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Personal Information has considerable market value.

83. Theft of PHI, in particular, is gravely serious: "Medical identity theft is when someone uses your personal information — like your name, Social Security number, health insurance account number or Medicare number — to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care. If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[25] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

84. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Personal Information and/or financial information is stolen and when it is

[25] *See* Federal Trade Commission, *Medical Identity Theft*. Available at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed May 3, 2022).

used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at 29.

85. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

86. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

87. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

88. Sensitive Personal Information can sell for as much as $363 per record according to the Infosec Institute.[26] PII is particularly valuable because criminals

[26] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed May 2, 2022).

can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

89. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[27] Such fraud may go undetected until debt collection calls commence months, or even years, later.

90. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[28]

91. Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

92. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are

[27] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed May 2, 2022).
[28] *Id.* at 4.

able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[29]

93. Data like a Social Security number, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[30]

Elderly Populations Are Reluctant to Change After a Data Breach

94. In 2020, the AARP sponsored Javelin Strategy Research to do a report on identity fraud strategies for Americans aged 55 years and older. While this report and its related research show that elders experience similar rates of being victims or identity fraud as the overall U.S. population, it also indicates certain troublesome patterns among this population, which includes a majority of the patients/residents at NHS.[31]

[29] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed May 2, 2022)

[30] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 2, 2022).

[31] Identity Fraud in Three Acts: A Consumer Guide, available at: https://www.aarp.org/content/dam/aarp/home-and-family/family-and-friends/2020/10/aarp-Identity-fraud-report.pdf, at 8 (last accessed May 2, 2022).

95. After being a victim of identity fraud, "[c]onsumers aged 65+ typically do not change how they shop, bank, or pay following a fraudulent event. A surprising 70% of consumers 65 and older exhibit reluctance to change familiar habits."[32] This reluctance increases the risks that elders face after a data breach like that at NHS.

96. For Americans 55+ years old, Javelin's research has shown that they are more likely to use identity theft protection, credit report security freezes, and credit monitoring than the overall U.S. population.[33]

97. Since elders are more likely to rely on the type of credit monitoring services that NHS has offered, albeit for only one year, and because many of the victims of the NHS Data Breach are likely to be over 55 years old, NHS's offer of a single year of free credit monitoring through Knoll is woefully inadequate. Their Personal Information is likely to be exploited for years, yet NHS's relief is limited.

Plaintiff's Experience

Plaintiff Shymikka Griggs

98. Plaintiff Shymikka Griggs is and at all times mentioned herein was an individual citizen residing in the State of Alabama, in the City of Birmingham, Jefferson County.

[32] *Id.* at 9.
[33] *Id.* at 8.

99. Plaintiff Griggs is a former employee of NHS Management, LLC. When she was initially employed by NHS, she was required to provide NHS with her Personal Information, including but not limited to her Social Security number.

100. On or about April 4, 2022, Plaintiff Griggs received a mailed Notice of Data Breach Letter, related to NHS's Data Breach that occurred between February 2021 and May 2021. Attached as Exhibit A.

101. The Notice Letter that Plaintiff Griggs received listed an extensive amount of her PII and PHI that "was accessible by an unknown actor as a result of this incident." The letter stated that the "accessible information" included her "name, date of birth, Social Security number, medical information, and health insurance information." See Exhibit A.

102. Plaintiff Griggs is alarmed by the amount of her Personal Information that was stolen or accessed, and even more by the fact that her Social Security numbers were identified as among the breached data on NHS's computer system.

103. Since NHS's Data Breach, Plaintiff Griggs has been notified by Credit Karma that her PII was found on 18 different sites on the "dark web." She has been working with Credit Karma to freeze her credit.

104. For a couple of months, Plaintiff Griggs has been receiving a significantly higher number of spam emails, calls, and texts. She now receives about three spam calls per a day.

105. Plaintiff Griggs has received several calls from the Apple fraud department asking whether she made certain Apple product purchases worth about $3000. She has not purchased any Apple products recently and explained that to Apple.

106. Since the NHS Data Breach, Plaintiff Griggs monitors her financial accounts more often. She spends about 15 minutes per day doing so, which is time that she cannot spend on activities she would prefer.

107. Plaintiff Griggs is aware that cybercriminals often sell Personal Information and that hers could be abused months or even years after the NHS Data Breach.

108. Had Plaintiff Griggs been aware that NHS's computer systems were not secure, she would not have entrusted NHS with her Personal Information.

109. Due to the Data Breach, Plaintiff Griggs anticipates spending time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

Plaintiff's and Class Members' Damages

110. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach and data breach.

111. Moreover, NHS has offered only a paltry one year of identity theft monitoring and identity theft protection through Kroll. This one-year limitation is inadequate when NHS's victims are likely to face many years of identity theft.

112. Furthermore, Defendant NHS's credit monitoring offer and advice to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, NHS expects Plaintiff and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

113. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI.

114. These services are also inadequate as NHS fails to acknowledge that many of the victims of its Data Breach are elderly or infirmed and may not be able to adequately protect themselves from fraud and identity theft.

115. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

116. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, credit card fraud, tax return fraud, medical services billed in their names, utility bills opened in their names, and similar identity theft.

117. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Personal Information.

118. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

119. Plaintiff and Class Members also suffered a loss of value of their Personal Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

120. Patient/resident Class Members and their family members or guardians were also damaged via benefit-of-the-bargain damages. Part of the price these Class Members paid to Defendant was intended to be used by Defendant to fund adequate

security of Defendant's computer property and Class Members' Personal Information. Thus, the Class Members did not get what they paid for. Specifically, they overpaid for services that were intended to be accompanied by adequate data security but were not.

121. Alternatively, Plaintiff and other employee/vendor Class Members were also damaged via benefit-of-the-bargain damages. Part of the wages or pay terms that these Class Members negotiated with Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiff's and Class Members' Personal Information. Thus, Plaintiff and the Class Members did not get the benefit of their bargain.

122. Plaintiff and Class Members have been damaged by the compromise of their Personal Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

123. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

124. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

125. In addition, many Class Members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

126. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, is encrypted, and that access to such data is password-protected.

CLASS ACTION ALLEGATIONS

127. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (the "Class" or "Classes").

128. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons whose Personal Information was compromised as a result of the Data Breach reported to HHS on or about October 29, 2021 by Defendant NHS (the "Class").
>
> Alabama Subclass
>
> A subclass of those Alabama citizens whose Personal Information was compromised as a result of the Data Breach reported to HHS on or about October 29, 2021 by Defendant NHS (the "Alabama Subclass").

129. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal

representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

130. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

131. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on NHS's report to HHS the Class consists of at least 501 individuals whose data was compromised in the Data Breach.

132. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personal Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Personal Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Personal Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant breached its duty to promptly notify HHS, Plaintiff, and Class Members of the Data Breach;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent, and;

k. Whether Plaintiff and Class Members are entitled to damages and/or injunctive relief.

133. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Personal Information, like that of every other Class Member, was compromised in the Data Breach.

134. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

135. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

136. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class

Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

137. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

138. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify HHS, Plaintiff, and the Class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant's failed to take commercially reasonable steps to safeguard consumer Personal Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

139. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count
Negligence
(On Behalf of Plaintiff and All Class Members)

140. Plaintiff realleges and incorporates by reference the allegations in paragraphs 1 to 138 above as if fully set forth herein.

141. Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Personal Information held

within it—to prevent disclosure of the information, and to safeguard the information from theft.[34]

142. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a cyberattack.

143. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

144. Defendant's duty of care to use reasonable security measures arose due to the special relationship that existed between it and the Class, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a cyberattack and data breach.

145. HIPAA imposes a duty and an actionable standard of care for an ordinary negligence claim. The HIPAA Privacy Rule prohibits covered entities

[34] *Wallace v. Health Quest Sys., Inc.*, No. 20 Civ. 545 (VB), 2021 WL 1109727, at *9 (S.D.N.Y. Mar. 23, 2021) (finding that plaintiff plausibly pleaded that an operator of hospitals and healthcare providers owed a duty of care to safeguard customers' and patients' sensitive personal information).

from using or disclosing personal health information except as permitted by regulation. 45 C.F.R. § 164.502(a). The HIPAA privacy restrictions also govern the business associates of covered entities. 45 C.F.R. § 160.102. NHS is subject to the actionable standards of care established by HIPAA as a business associate of covered entities.

146. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

147. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

148. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also

because Defendant was bound by industry standards to protect confidential Personal Information.

149. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant includes, but is not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Personal Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Personal Information;

e. Failing to detect in a timely manner that Class Members' Personal Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

150. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. The breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in both the financial services and medical industry.

151. The Data Breach was foreseeable due to Defendant's to adequately safeguard Class Members' Personal Information and was foreseeable that it would result in one or more types of injuries to Class Members.

152. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

153. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Second Count
Negligence Per Se
(On Behalf of Plaintiff and All Class Members)

154. Plaintiff realleges and incorporates by reference the allegations in paragraphs 1 to 138 above as if fully set forth herein.

155. Pursuant to the HIPAA (42 U.S.C. § 1302d et seq.) and the FTCA, NHS was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

156. NHS breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

157. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to NHS's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Personal Information.

158. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to NHS's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

159. NHS's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information.

160. Plaintiff and Class Members have suffered and will continue to suffer damages as a result of NHS's conduct. Plaintiff and Class Members seek damages and other relief as a result of NHS's negligence.

Third Count
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

161. Plaintiff realleges and incorporates by reference the allegations in paragraphs 1 to 138 above as if fully set forth herein.

162. NHS provides medical services, employment, and/or vendor sales to Plaintiff and Class Members. Plaintiff and Class Members also formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for medical goods and services and/or receiving pay for labor or goods from Defendant.

163. Through Defendant's performance of, sale of, and/or purchase of medical goods and services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Personal Information in accordance with NHS's policies, practices, and applicable law.

164. As consideration, Plaintiff and Class Members paid money to NHS and/or their insurers for medical services, or alternatively, provided labor or products, and turned over valuable PII and PHI to Defendant. Accordingly, Plaintiff

and Class Members bargained with NHS to securely maintain and store their Personal Information.

165. NHS violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

166. Plaintiff and Class Members have been damaged by NHS's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

Fourth Count
Invasion of Privacy
(On Behalf of Plaintiff and All Class Members)

167. Plaintiff realleges and incorporates by reference the allegations in paragraphs 1 to 138 above as if fully set forth herein.

168. Plaintiff and Class Members maintain a privacy interest in their Personal Information, confidential information that is also protected from disclosure by applicable laws set forth above. Plaintiff and Class Members' Personal Information was contained, stored, and managed electronically in Defendant's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive,

confidential matters regarding Plaintiff's and Class Members' identities, unique identification numbers, medical histories, and financial records that were only shared with Defendant for the limited purpose of obtaining and paying for healthcare, medical goods and services, or alternatively, exchanged labor or products for pay from Defendant. Additionally, Plaintiff's and Class Members' Personal Information, when contained unencrypted and in electronic form, is highly attractive to criminals who can nefariously use their Personal Information for fraud, identity theft, and other crimes without their knowledge and consent.

169. NHS's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person.

170. NHS's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' personal quarters where their Personal Information was stored and disclosed private facts about their health and finances into the public domain.

171. Plaintiff and Class Members have been damaged by NHS's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

Fifth Count
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

172. Plaintiff realleges and incorporates by reference the allegations in paragraphs 1 to 138 above as if fully set forth herein.

173. Plaintiff and Class Members conferred a benefit on NHS by paying for data and cybersecurity procedures to protect their Personal Information that they did not receive.

174. NHS has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to NHS's conduct alleged herein, it would be unjust and inequitable under the circumstances for NHS to be permitted to retain the benefit of its wrongful conduct.

175. Plaintiff and the Class Members are entitled to full refunds, restitution and/or damages from NHS and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by NHS from its wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation may be created.

176. Additionally, Plaintiff and the Class Members may not have an adequate remedy at law against NHS, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

Sixth Count
Breach of Confidence
(On Behalf of Plaintiff and All Class Members)

177. Plaintiff realleges and incorporates by reference the allegations in paragraphs 1 to 138 above as if fully set forth herein.

178. At all times during Plaintiff's and Class Members' interaction with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Personal Information.

179. As alleged herein and above, Defendant's relationship with Plaintiff's and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

180. Plaintiff and Class Members provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit Personal Information to be disseminated to any unauthorized parties.

181. Plaintiff and Class Members also provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect such Personal Information from unauthorized disclosure.

182. Defendant voluntarily received in confidence Plaintiff's and Class Members' Personal Information with the understanding that it would not be disclosed or disseminated to the public or any unauthorized third parties.

183. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' Personal Information, Plaintiff's and Class Members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

184. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

185. But for Defendant's disclosure of Plaintiff's and Class Members' Personal Information in violation of the parties' understanding of confidence, their protected Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected Personal Information, as well as the resulting damages.

186. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Personal Information.

187. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching to prevent, detect, contest, and recover from medical fraud, financial fraud, and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of past and current patients/residents and their families and/or guardians, employees, vendors in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

188. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

Seventh Count
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

189. Plaintiff realleges and incorporates by reference the allegations in paragraphs 1 to 138 above as if fully set forth herein.

190. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship, as a consequence of the special relationship of trust and confidence that exists between patients/residents and their families and/or guardians, employees, vendors (like Plaintiff and Class Members) and businesses like Defendant, that provide medical care, housing, treatment, and/or employment.

191. In light of their special relationship, Defendant has become the guardian of Plaintiff's and Class Members' Personal Information. Defendant has become a fiduciary, created by its undertaking and guardianship of the Personal Information, to act primarily for the benefit of their patients/residents and employees, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' Personal Information and to timely notify them in the event of a data breach.

192. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

a. properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' PII and PHI;

b. timely notify Plaintiff and Class Members of the Data Breach;

c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

e. implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);

f. to identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

g. to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94);

j. improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

k. effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5)

l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c); and

m. otherwise failing to safeguard Plaintiff's and Class Members' Personal Information.

193. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Personal Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the Plaintiff and Class Members.

194. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages and compensatory damages in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: May 4, 2022

Respectfully submitted,

/s/ *Taylor C. Bartlett*

HENINGER GARRISON DAVIS LLC
Taylor Bartlett
2224 1st Avenue N.
Birmingham, AL 35203
Tel: 205.326.3336
Fax: 205.380.8085
Taylor@hgdlawfirm.com

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for Plaintiff

**pro hac vice to be filed*